REMARKS

This Amendment is in response to the non-final Office Action of April 27, 2010 in which claims 1-32 were rejected.

As mentioned in the first full paragraph on page 2 of the remarks section of the pre-appeal brief request for review filed May 21, 2009, the subject matter of independent method claim 1 can best be understood by viewing the claim alongside applicant's Fig. 2 where a secure channel 207 is shown connecting a server 208 to an installation part 203 of an application 202 and connecting the installation part 203 to a secure environment 205 and the device 201. The device 201 may be a terminal device as claimed in claim 1 and receive a first key in its secure environment 205 via the secure channel 207 from the server 208 outside the terminal 201. The first key is for decrypting an encrypted application 204. The secure channel 207 may for example (as discussed in the specification) involve the server 208 encrypting the first key with a public key of device 201. It is also possible to for instance use the SSL protocol to transfer the first key into the secure environment 205. See page 3, paragraph 0028 in the right-hand column at lines 14-23 (corresponding to the as-filed specification at page 10, lines 20-30).

Regarding the obviousness rejection of claims 1-3, 8-10 and 22-28 based on *Cassagnol et al* (U.S. 2002/0129245) in view of *Audebert et al* (U.S. 2003/0108204), the paragraph 0012 in *Cassagnol et al* at page 2 thereof does not disclose the first limitation of claim 1, contrary to the Examiner's allegation. For instance, paragraph 0012 merely states that there is a cipherer (see for instance Fig. 2 at reference numeral 20 and also the same reference numeral in Fig. 3) which re-encrypts decrypted, re-authenticated information such that it differs from its original encrypted form to mask modification information. As known in the art, such masking to hide modification information is accomplished with whitening keys. There is no disclosure whatsoever in paragraph 0012 that the first whitening key used to decrypt the encrypted information imported from the external memory in a first form is received via a secure channel. There is also nothing about a server, as

admitted by the Examiner, and furthermore there is nothing disclosed about an application.

As pointed out in the present specification at page 2, lines 28-30, application providers have vary limited possibilities to define the way the application is handled during application installation (see the last three lines of published paragraph [0006] at page 1 of the applicant's own publication US 2004/0176068 A1). To emphasize this feature, the "receiving" limitation of claim 1 has been amended to make it clear that when the application is received in the terminal, a first key is received via a secure channel into a secure environment of the terminal. See page 4, lines 22-26 or the corresponding text at published paragraph [0013] lines 13-16 for support.

Thus, the first limitation of claim 1 is now more clearly distinguished from the key-cycling and/or cycling of the whitening key to mask modification information as set forth in paragraph [0012] on page 2 of the *Cassagnol et al* reference.

Regarding the second, "decrypting" limitation of claim 1, the Examiner points to *Cassagnol et al* at paragraph [0025] at the top of the left hand column of page 3. In that paragraph, the decryption of the imported information in the first form is discussed as being carried out by the cipherer and encrypted into a second form different from the first form when exported as discussed above in connection with paragraph [0012]. Since there is no first key disclosed as having been received from a server in the secure environment of *Cassagnol et al*, as discussed in the preceding paragraph above, then there can be no decrypting in the secure environment of anything by means of the absent first key from a server. The only thing disclosed in paragraph [0025] is that there are first and second whitening keys but it does not say where they come from except suggesting that there is a random number generated that generates the second whitening key without saying anything at this point about where the first key comes from, much less that it comes from a server. It is however stated in paragraph [0085] at the top of the right hand column on page 9 that the whitening keys are generated within the device itself by means of the entropy source 48 (see Fig. 3). The source of the whitening keys is clearly not from a server but from within the device 10 of *Cassagnol et al* itself. Any storage

thereof (in a secure way) in the external memory 24 for later retrieval would be done because of a lack of storage space in the secure environment (see paragraph [0058] on page 6). Later retrieval thereof would not be from a server. Therefore, it is incorrect for the Examiner to state that *Cassagnol et al* shows either receiving a first key from a server or decrypting anything by means of said first key.

The Examiner admits there is no server and no secure channel but cites the newly applied *Audebert et al* reference for showing these. See secure sending 375 in Fig. 3B of replacement keys. The secure transmission of the *Audebert et al* reference, however, doesn't have anything to do with decrypting an encrypted application. Rather, it has to do with key replacement and these is no motivation to combine, at least not for the reason given by the Examiner because the *Cassognol et al* reference already shows a Network 128 in Fig. 5 and there is no need or reason necessary to provide the replacement keys of the *Audebert et al* reference or to replace the Network 128 of *Cassagnol et al*.

The above comments made with respect to claim 1 apply equally to independent claims 2, 8, 9, and 22 and, for at least the same reasons, their dependent claims 3, 10, and 23-28 rejected on the same ground. Withdrawal of the obviousness rejection of claims 1-3, 8-10 and 22-28 is requested.

Regarding the obviousness rejection beginning in Section 17 on page 9, these dependent claims are nonobvious for at least the same reasons as advanced above in connection with Applicant overcoming the obviousness rejection of their respective independent claims and withdrawal thereof is requested.

Regarding the obviousness rejection beginning in Section 30 on page 13, these dependent claims are nonobvious for at least the same reasons as advanced above in connection with Applicant overcoming their respective independent claims. Withdrawal of the obviousness rejection of claims 7, 14, 18, 21 and 29-32 is requested.

The objections and rejections of the Office Action of April 27, 2010, having been obviated by amendment or shown to be inapplicable, withdrawal thereof is requested and passage of claims 1-32 to issue is solicited.

Respectfully submitted,

/Francis J. Maguire/

Francis J. Maguire
Attorney for the Applicant
Registration No. 31,391

FJM/mo
Ware, Fressola, Van Der Sluys & Adolphson LLP
755 Main Street, P.O. Box 224
Monroe, CT 06468
(203) 261-1234